



DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MEDICAL DEPARTMENT CENTER AND SCHOOL
AND FORT SAM HOUSTON
2250 STANLEY ROAD
FORT SAM HOUSTON, TEXAS 78234-6100

REPLY TO
ATTENTION OF
IMSW-SMH-IM

11 JUL 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Installation Information Management Policy 25-01, Use of Federal Government Communications Systems and Resources

1. REFERENCE. AR 25-1, Army Knowledge Management and Information Technology , 15 July 2005, Chapter 6, 15 July 2005 and AR 25-2, Information Assurance, 14 November 2003.
2. PURPOSE. The purpose of this memorandum is to provide reinforcement of the Army and local policy on use of Federal Government communications systems and resources.
3. SCOPE. This policy applies to all organizations and units located on or supported by Fort Sam Houston, Camp Bullis, and Camp Stanley, and that have connectivity to the installation network managed by the Director of Information Management (DOIM). This policy applies to both Government-owned and leased automation equipment.
4. BACKGROUND. The reference states, "The use of DoD and other Government telephone systems, e-mail and other systems (including the Internet) are limited to the conduct of official business or other authorized uses." The reference also states, "Users will not install new software packages, software upgrades, free software, freeware, shareware, etc., without the authorization of their systems administrator. Unauthorized software may contain harmful viruses or defects which can result in the loss of data or system failure." The DOIM/ITT is the "systems administrator."
5. POLICY. Current local policy does permit limited personal use of Government Internet and email resources. Such use must be before or after work, or during lunch or other authorized breaks during the workday. This permission does not extend to communications in support or furtherance of private business enterprises, or any other use that would reflect adversely on the Department of Defense. In the recent past, users trying to do official business during normal work hours (0700-1600) have experienced access speeds that are unacceptably slow because of the use of unauthorized applications. Examples of such applications are programs that use

IMSW-SMH-IM

SUBJECT: Installation Information Management Policy 25-01, Use of Federal Government Communications Systems and Resources

excessive bandwidth such as Peer to Peer software including Napster and Gnutella; streaming radio, video, and television; Weatherbug; and Realplayer. These and similar programs are not authorized for use on the installation network at any time and excessive, unauthorized bandwidth users will be reported to the chain of command for disciplinary actions.


6. The use of Personal Owned Systems is prohibited from using the Fort Sam Houston Network resources. Systems found using the Federal Government resources will have their systems confiscated, investigated and appropriate legal actions will be initiated by the applicable chain of command.

7. Systems not managed by the Fort Sam Houston's DOIM but using the Fort Sam Houston's network resources will require an in-depth security review and approval by the local Designated Approval Authority (DAA). These systems will be revalidated annually.

8. The reference also states, "All information, including personal information placed on or sent over DOD computer systems may be monitored." The DOIM will continue monitoring the Fort Sam Houston network and will delete any unauthorized software applications and block any unauthorized or questionable web sites. All incidents found will be sent through the applicable chain of command for appropriate action.

9. This policy will be reviewed 2 years from the implementation date.

10. The point of contact is Mr. Jack D. Poland, Director of Information Management, 221-1300/5281, or email address jack.poland1@us.army.mil.


RUSSELL J. CZERW
Major General, DC
Commanding

DISTRIBUTION:
A & B